Document created: 2 March 99

Information Assurance – the Achilles' Heel of Joint Vision 2010?

CDR Sam Cox, USN
MAJ Ron Stimeare, USA
MAJ Tim Dean, USA
Maj Brad Ashley, USAF

Armed Forces Staff College
Joint and Combined Staff Officer School
Intermediate Course 98-3

Faculty Advisor
Jerry Mitchell
Seminar 7

Thesis Statement

Information Assurance is the Achilles' Heel of Joint Vision 20 10.

Abstract

In this paper, we will discuss Joint Vision 20 10, Information Operations/Information Assurance, the cyber threat, three Information Assurance examples, and findings from recent studies. Finally, we will make specific recommendations on what DoD should do to remedy this Achilles' Heel and make Joint Vision 20 10 a viable concept.

Introduction

In July 1996, the Chairman of the Joint Chiefs of Staff published his vision of how the U.S. military will prepare to meet the challenges of an uncertain future. Entitled Joint Vision 20 10 (JV2010), this document identifies four "new" operational concepts that, if mastered, will allow the U.S. military to engage in "decisive operations" and succeed in any mission at any level of war from peace operations through nuclear war. The four new operational concepts that will enable the U.S. to achieve "full spectrum dominance" are: "dominant maneuver, precision engagement, full dimensional engagement, and focused logistics." [1] The key enabler for all four of these operational concepts is "information superiority" based on the ongoing revolution in technological development. Without information superiority, JV20 1 O's new concepts become little more than the current operational concepts of maneuver, strike, protection and logistics. In short, without information superiority, the U.S. military will lose its edge and find itself fighting the protracted wars of attrition JV2010 is designed to preclude.

Information superiority is defined as "the capability to collect, process, and disseminate an uninterrupted flow of information, while exploiting or denying an adversary's ability to do the same."[2] Thus, by defmition, information superiority has both defensive and offensive implications. In order to achieve an uninterrupted flow of information, the systems and processes that enable that flow must be defended against adversarial actions. Although degrading an adversary's information flow is important, defending one's own is even more critical to successful military operations.

The DoD infrastructure consists of over 2.1 million computers, 10,000 local area networks, and 1000 long distance networks.[3] JV2010 drives efforts to further interconnect these systems and migrate toward a network centric environment.[4] Over 95% of DoD's systems utilize public communications networks

Form SF298 Citation Data

Report Date *("DD MON YYYY")* 02031999	**Report Type** N/A	**Dates Covered (from... to)** *("DD MON YYYY")*

Title and Subtitle Information Assurance - the Achilles Heel of Joint Vision 2010?	**Contract or Grant Number**
	Program Element Number
Authors	**Project Number**
	Task Number
	Work Unit Number
Performing Organization Name(s) and Address(es) Armed Forces Staff College Joint and Combined Staff Officer School	**Performing Organization Number(s)**
Sponsoring/Monitoring Agency Name(s) and Address(es)	**Monitoring Agency Acronym**
	Monitoring Agency Report Number(s)
Distribution/Availability Statement Approved for public release, distribution unlimited	
Supplementary Notes	
Abstract	
Subject Terms "IATAC COLLECTION"	
Document Classification unclassified	**Classification of SF298** unclassified
Classification of Abstract unclassified	**Limitation of Abstract** unlimited
Number of Pages 12	

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	3/2/99	Report

4. TITLE AND SUBTITLE
Information Assurance - The Achilles' Hell of Joint Vision 2010

5. FUNDING NUMBERS

6. AUTHOR(S)
CDR Sam Cox, USN, MAJ Ron Stimeare, USA, MAJ Tim Dean, USA, Maj Brad Ashley, USAF

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
IATAC
Information Assurance Technology Analysis Center
3190 Fairview Park Drive
Falls Church VA 22042

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Defense Technical Information Center
DTIC-IA
8725 John J. Kingman Rd, Suite 944
Ft. Belvoir, VA 22060

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION / AVAILABILITY STATEMENT

12b. DISTRIBUTION CODE
A

13. ABSTRACT ***(Maximum 200 Words)***
In this paper, we will discuss Joint Vision 20 10, Information Operations/Information Assurance, the cyber threat, three Information Assurance examples, and findings from recent studies. Finally, we will make specific recommendations on what DOD should do to remedy this Achilles' Heel and make Joint Vision 20 10 a viable concept.

14. SUBJECT TERMS
Joint Vision 2010,

15. NUMBER OF PAGES

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	UNCLASSIFIED	UNCLASSIFIED	None

available to the general public. These networks are classified as the global, national, and defense information infrastructures (GII, NII, and DII). Although these names imply independence, they all use interconnected transport medium linked to public switches that route data between geographically separated systems. This includes DoD's classified systems that operate on the Secret Internet Protocol Routing Network or SIPRNET. The multitude of automated systems allows DoD to command, control, protect, pay, supply, and inform the force. As dependence on increasingly interconnected information systems grows, so does DoD's vulnerability.

What is IO/IA?

The process of attacking and defending information is Information Operations (IO), defined as "action taken to affect adversary information and information systems while defending one's own information and information systems."[5] This definition communicates that there is more to IO than simply attacking computer systems. IO consists of technology, processes, and human factors impacting the mind of the decision maker. IO can be targeted against leaders or key decision makers, but can also affect every echelon of the military, government, and even the general population.

Defensive Information Operations "ensure timely, accurate, and relevant information access while denying adversaries the opportunity to exploit friendly information and information systems for their own purposes."[6] Defensive IO are conducted through Information Assurance (IA), Operational Security (OPSEC), physical security, counter deception, counter psychological operations, counter intelligence, electronic warfare, and special information operations.[7] Although each of these actions is important, Information Assurance is the most critical to the success of the new operational concepts described in JV2010 because it ensures that friendly systems will provide the information as required. IA is vital because of the rapidly continuing technological advances in systems (particularly in the speed, processing power and miniaturization of computers) that enable the information revolution, which is vital to the success of JV2010.

Information Assurance is defined as "information operations that protect and defend information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities? The Information Assurance process ensures that: authorized users have guaranteed access to appropriate friendly information systems (availability;) friendly information systems are protected from unauthorized change or tampering (integrity;) authorized users are verified (authentication;) the information within the system is protected from unauthorized disclosure (confidentiality;) and friendly information systems provide an undeniable record of proof of user participation and transactions (non-repudiation.) Any information system or process that lacks any of the above information assurance components is vulnerable to adversary disruption or exploitation and must be considered unreliable.

The Target

Combating unauthorized access to DoD computer systems is a daily battle. The 1998 joint FBI and Computer Security Institute's (CSI) survey of 520 security practitioners in the U.S. reveals computer crime and security breaches have increased by over 16% since 1997.[9] The explosion of such information attacks is indicative of the ease with which intrusions are perpetrated today. As intrusions continue to rise, U.S. joint forces may be hindered from accomplishing their tasks, seriously degrading the warfighting CINC's ability to accomplish the mission, and adversely affecting U.S. national security.

What damage can information attacks cause?

The potential for damage to national security interests from offensive IO targeted at DoD systems is only limited by the skill and imagination of the intruder. Several techniques, such as denial of service, injection, theft, destruction, and spoofing, may be combined to cause significant disruption or delay of military operations.

Denial of Service (DOS) attacks are characterized by intruders obstructing access to a computer system from one or more authorized users. The damage done to national security interests by such attacks depends on the functions of the actual system attacked. Injection or modification of data may be accomplished by unauthorized agents to mislead decision makers. Injection or modification of data is typically more difficult to detect and potentially more dangerous than a denial of service attack.

Theft and / or destruction of data accomplished by unauthorized attackers may be harmless or may have severe national security implications. Theft of personal information may permit attackers to assume the electronic identity of key officials allowing them to send messages, including directives, to decision makers and operators to initiate undesirable military actions.

Who are these information warriors and why do they attack?

The diversity of information operation adversaries ranges from individuals to nation-states. Their motivations include innocent curiosity, challenge, bravado, revenge, embarrassment, greed, idealistic activism, and national security interests. U.S. adversaries are conducting information operations against us daily. Hackers are probing while well-organized and resourced foreign intelligence collection efforts are performing an intelligence preparation of the cyber battlefield to gain unauthorized knowledge and access to DoD systems.

An internal threat from disaffected DoD employees with authorized access to defense information systems comprises another large pool of potential information adversaries. The damage such individuals are capable of today is exponentially higher than was possible before reliance on computerized information systems. 44% of respondents to the 1998 CSI/FBI Computer Crime and Security Survey reported unauthorized access by employees. This figure exceeded all other reported intrusions and continues to be DoD's number one threat.[10] Also, insiders are prime candidates to be "hired" by potential adversaries.

The typical "innocent juvenile hacker" who intrudes on systems for sport is nonetheless a potential threat to national security. The danger in attributing most detected intrusions to harmless hackers is to minimize the seriousness of the potential consequences. Hackers often use their age or status as a screen when, in fact, they may be "coached", persuaded or even hired for financial gain by anonymous agents that have more sinister motives. Computer vandals are a more serious type of hacker whose motivations are simply to break into computers to wreak havoc and cause damage.

Subnational groups or terrorist organizations with political agendas not aligned with U.S. interests pose a more persistent threat than all but nation-state supported intruders. They may cheaply and anonymously gather information to embarrass or target DoD vulnerabilities. Corporate or national competitors and professional thieves pose an industrial espionage threat to defense contractors working for DoD. The costs of developing advanced conventional weapons systems are high. A poorly funded adversary, or even an ally, may derive financial and tactical advantages by exploiting industrial secrets funded by DoD.

What are the information warrior's weapons?

Cyber warrior weapons are often readily available for download on the Internet. Unlike the tools of conventional warfare, the tools of this trade require no long term acquisition, training, and fielding process to mount an attack. As the typical PC has become more powerful and easier to use, so has the sophistication of the weapons that information adversaries have at their disposal. A comparatively low technology adversary with minimal funding, training, manning, and defense infrastructure is capable of employing these weapons on short notice from anywhere in the world. One key advantage afforded the information warrior is freedom from the burden of time and money needed to field and project a conventional force.

One common method to gain unauthorized access is through the normal log-on process from the command line prompt of a telnet or remote login session. User names and passwords may be gleaned from any number of methods. Free password cracking software is available on the Internet for anyone

wishing to test the security of (or break into) networked systems. Once logged onto a system as a valid user an attacker may read, copy, delete, substitute, and modify data and programs on the host. Other computer vulnerabilities are easily found on the Internet to include exploitation tools.

Given access to a target system the cyber warrior may inject, load, or install a program or script on the machine. Such programs may reside on the machine indefinitely if undetected, quietly gathering key information such as user names and passwords. They may provide backdoors to the systems for later entry at a time of the attacker's choosing. Trojan horse programs are seemingly legitimate operating system utilities or programs substituted by attackers for the real programs. Users run trojan horses believing they are real programs deriving expected results while unknown to them, additional malicious or destructive code executed in the background of the expected process is performing unintended tasks without user knowledge.

Toolkits are neatly bundled packages containing many of the above mentioned tools. They commonly incorporate easy to learn graphical (point and click) user interfaces. The danger of the proliferation of such tools is in the increased amount of damage a single attacker or organized group of attackers may inflict. These tools provide the attacker anonymity and hinder trace actions.

The following three cases from the past four years illustrate DoD's vulnerability: Rome Labs, ELIGIBLE RECEIVER, and SOLAR SUNRISE.

Rome Labs-March 1994

The Rome Labs computer intrusion case is one of the most famous and most documented attacks on DoD computer networks. In March 1994, two hackers successfully attacked Rome Labs at Griffis Air Force Base, New York over 150 times during a 26 day period. Rome Labs was the Air Force's premiere command and control research center for artificial intelligence, radars, and target detection/tracking systems. The hackers used Rome Labs computers as a launching point for subsequent attacks on over 100 other Air Force, Navy, NASA, and commercial systems across the country. [11,12]

Rome Labs was first compromised on 23 March 1994 but was not discovered five days later. The attackers installed an illegal computer wiretap program called a "sniffer", which captures valid logons and passwords, and subsequently captured over 100 additional user accounts. E-mails were read, copied, and deleted and megabytes of data were downloaded from penetrated systems. Penetrated systems included: Rome Labs, commercial Internet service providers, HQ NATO, Goddard Space Center, Jet Propulsion Lab, National Aerospace Plan Joint Program Office, Wright-Patterson AFB, missile contractors, and numerous U.S. Army sites. Foreign countries used in attempts to hide the hackers' activities included: U.S., the UK, Colombia, Chile, Latvia, and South Korea. [13,14]

The attackers used the Rome Labs' computers to download megabytes of Korean Atomic Research Institute information and, due to the vast amounts of data, even stored this information on the Rome Labs' servers. At the time, it was unclear whether the data was being copied from North or South Korea. Korea could have seen this transfer and storage of their research information as an intrusion by the USAF, or even perceived it as an aggressive act of war. In 1994, the U.S. was undergoing tenuous negotiations with North Korea on their nuclear programs. The stolen data luckily turned out to be from South Korea. The Government Accounting Office (GAO) estimated total costs of the Rome Labs incident at $500,000 not including the cost of the U.S. research data that was compromised. It is extremely difficult to quantify the loss from a national security point of view. [15,16]

Who were these attackers that nearly had international conflict implications? A sixteen year-old from the U.K. entered a plea bargain and paid a $1900 fine while another twenty-two year old pled not guilty and was acquitted on all charges in February 1998. The 16 year old was operating on a home computer in his parents' house and had a "C" grade average in his high-school computer class. [17,18]

ELIGIBLE RECEIVER 1997, (9-13 June 1997)

ELIGIBLE RECEIVER (ER) '97 was a no-notice Joint Staff Exercise designed to test DoD planning

and crisis action capabilities when faced with attacks on DoD information infrastructures. This exercise revealed significant vulnerabilities in DoD information systems and specific deficiencies in responding to attacks on their information systems. ER '97 involved DoD, Joint Staff, the Services, USACOM, USPACOM, USSPACECOM, USSOCOM, USTRANSCOM, NSA, DISA, NSC, DIA, CIA, FBI, NRO, and the Departments of State, Justice, and Transportation.

ER '97 included an actual attack on key DoD information systems. Known vulnerabilities were exploited and computer systems were actually disrupted. DoD Red Team computer experts derived techniques and tools from open source research (primarily from the Internet), used commercial internet accounts, and exploited actual vulnerabilities. Their targets included: the National Military Command Center (NMCC) in the Pentagon, USPACOM, USSPACECOM, USTRANSCOM, and USSOCOM. The Red Team intruded computer networks, denied services, changed/removed/read e-mails, and disrupted phone services. The team gained super-user access in over 36 computer systems which meant they could create new accounts, delete accounts, turn the system off, or reformat the server hard drives. The key observations of the exercise included:

- poor informational/operational security practices contributed to DoD vulnerabilities
- attribution of attacks is very difficult (determining who and why)
- DoD has little capability to detect or assess cyber attacks
- detection, reporting, response processes are unresponsive to speed of cyber attacks. [19]

ER '97 demonstrated, in a real world exercise, that DoD is not properly organized for IO and cannot detect/report/respond to IO attacks in a timely manner. The Red Team attackers successfully demonstrated that, by using open source vulnerabilities and exploitation tools and techniques (readily available on the Internet), DoD networked computer systems can be severely degraded.[20]

SOLAR SUNRISE-February 1998

"I would characterize it [DoD computer network attacks] as being systematic and moderately sophisticated... I think this was, more than anything, a serious wake-up call."[21]

- John J. Hamre, Deputy Secretary of Defense

SOLAR SUNRISE was a series of DoD computer network attacks which occurred from l-26 February 1998. The attack pattern was indicative of a preparation for a follow-on attack on the DII. DoD unclassified networked computers were attacked using a well-known operating system vulnerability.[22] The attackers followed the same attack profile: (a) probing to determine if the vulnerability exists, (b) exploiting the vulnerability, (c) implanting a program (sniffer) to gather data, and (d) returning later to retrieve the collected data.

At least eleven attacks followed the same profile on Air Force, Navy, and Marine Corps computers worldwide.[23],[24] Attacks were widespread and appeared to come from sites such as: Israel, the United Arab Emirates (UAE), France, Taiwan, and Germany. The attacks targeted key parts of the defense networks and obtained hundreds of network passwords. Although all DoD targeted systems were reported as unclassified, we must remember many key support systems reside on unclassified networks (Global Transportation System, Defense Finance System, medical, personnel, logistics, and official e-mail).

DoD established a 24-hour emergency watch, installed intrusion detection systems on key nodes, and assisted law enforcement in computer forensics and investigation. SOLAR SUNRISE confirmed earlier ELIGIBLE RECEIVER findings: DoD has no effective indications and warning system, intrusion detection systems are insufficient, DoD is not organized effectively for IO, and that identifying the threat group and motives is a problem.[25] We need more trained personnel for our response teams, must develop a quick detect/report/response capability, and we must develop more automated intrusion detection capability.[26]

These attacks occurred when the U.S. was preparing for potential military action against Iraq due to UN weapons inspection disputes and could have been aimed at disrupting deployments and operations.[27] So who was behind these attacks-Iraq, terrorists, foreign intelligence services, nation states, or hackers for hire? The attackers were two teenagers from California and one teenager from Israel.[28],[29] Their motivations were ego, power, and the challenge of hacking into U.S. DoD computer systems.[30] We began the SOLAR SUNRISE description by stating that the attacks occurred on unclassified DoD systems. One of the California teenagers additionally admitted to penetrating computer networks at Lawrence Livermore Labs (a national nuclear research facility) and claims it was a classified system and that the FBI was extremely interested in his involvement with this site.[31] Total costs for the investigation, data recertification, cleansing infected systems of possible malicious code, trojan horses, and backdoors has yet to be accurately calculated for these attacks. The attacks did not cause any serious damage to DoD systems, however they could have severely impacted DoD during heightened tensions with Iraq.

The Rome Labs Case, ER '97, and SOLAR SUNRISE demonstrated the vulnerabilities of DoD computer networks. As Dr. Hamre, Deputy Secretary of Defense, said, "this should serve as a serious wake-up call".[32] If high-school kids can infiltrate DoD systems with ease, imagine the damage that could be done to U.S. security by skilled professionals or potential adversaries in future asymmetric conflicts.

Findings

"... the struggle for power changes when knowledge about knowledge becomes the prime source of power"

– Alvin Toffler

These documented cases illustrate DoD's need to make some changes in its approach to Information Assurance. DoD must act now to protect the security of its future. DoD needs to analyze, adapt and implement the recommendations from recently published Information Warfare Studies with specificity and expediency. If we do not, we will lose the advantage over our enemies and be studying this issue alone, isolated and by candlelight. We will have allowed the hackers of this world to destroy, disrupt and manipulate, at will, our communications, power and transit systems. As concluded in the 1997 President's Commission on Critical Infrastructure Protection, "Waiting for disaster will prove as expensive as it is irresponsible".

In November 1996, the Defense Science Board (DSB) published a report on Information Warfare (Defense). Their findings by and large matched those of "The President's Commission on Critical Infrastructure Protection" study, and several prominent National Defense University (NDU) articles such as: "Defensive Information Warfare"; "The Unintended Consequences of Information Age Technologies"; "Sun Tzu and Information Warfare". For the third year in a row, the DSB concluded that there is a need for extraordinary action to deal with the present and emerging challenges of defending against possible information attacks. These attacks could be on facilities, information, information systems, and networks of the United States which would seriously affect the ability of the DoD to carry out its assigned missions and functions.[33] They observed an increasing dependency on the DII and increasing doctrinal assumptions regarding the continued availability of that infrastructure.[34] These dependencies and assumptions are ingredients of a recipe for a national security disaster.[35] DoD cannot afford to sit by and wait for an "Electronic Pearl Harbor" before taking action.

Accordingly, the DSB recommended over 50 actions designed to better prepare the DoD for this new form of warfare.[36] Of the 13 major DSB recommendations, we feel five are essential to the immediate successful protection of the Joint Vision 20 10 Achilles' Heel:

1) Designate an accountable IO focal point. This was the DSB's most important recommendation. The Secretary of Defense must have a single focal point charged to

provide leadership of the complex activities and interrelationships that are involved in this new warfare area.[37]

2) Organize for IO - Defense (IO-D). This recommendation identifies the need for specific IO-D capabilities and organizations to provide or support the capabilities.[38]

3) Increase awareness. The DSB strongly suggests the need to make senior-level government and industry leaders more aware of the vulnerabilities and implications.[39]

4) Staff for success. A cadre of high-quality, trained professionals with recognized career paths is an essential ingredient for defending present and future information systems.[40]

5) Provide the resources. DSB estimated achieving its 13 Imperatives would cost approximately $3.1 billion over fiscal years 1997 through 2001.[41]

The Army has developed a three phased Network Security Improvement Program (NSIP) to implement these recommendations. Phase 1 contains low-cost actions that form the foundation for a solid information assurance program. These actions include assigning responsibilities, ensuring network integrity, and providing essential training.[42] Phase 2 of the Army plan is a mid-term strategy starting in June 1998. This phase consists of low to moderate cost actions and the continuation of Phase 1 actions. These phased actions have the affect of hardening the installation infrastructure. The goal is to identify and implement actions that require investment resources, such as automated intrusion detection systems (IDS). Phase 3 of the NSIP strategy begins the far-term actions, which will start in September 1998. Phase 3 includes continuation of Phases 1 and 2 actions and the installation of firewalls for specific network security requirements.[43]

The Air Force and Navy are developing their own plans in the absence of a single agency consolidating service efforts. The Air Force has its "Professionalization of Networks" concept which includes: creating a specific IO career path for both officers and enlisted personnel, incentives to remain in the military, highly technical training, and developing a security conscious cadre of professionals. The Air Force is ahead of the other services in deploying IDS. The Navy's concept is to protect their ships first and protect their land based systems second. They currently fall somewhere between the Air Force and the Army on IO preparedness. The services are fielding a wide variety of IDS, unilaterally setting detection features, and reporting differently. DOD must appoint an IO integrator for all the services to ensure synergy is achieved, as opposed to redundant parallel efforts and suboptimization, otherwise, efficiencies will not be realized and "risks accepted by one, will be shared by all". This cannot be tolerated in the JV2010 sophisticated network centric environment.

Recommendation

DoD must act now to make IA a top priority. This can only be accomplished by designating a single focal point for DoD, increasing training, budgeting for success, aggressively fixing our known vulnerabilities, as well as improving our detect/report/respond processes.[44]

Conclusion

Information Assurance is the Achilles' Heel of Joint Vision 2010. This statement is supported by the evidence presented in this paper: the President's Commission Report, the DSB findings three years in a row, and the three real world examples cited (each of which could have had far reaching international security implications). Increased deployment and use of information systems creates dependencies which in turn increase our vulnerability to attack. All that is required to attack DoD computers today is a home computer, access to the Internet, and a little ingenuity.

IA must be a top priority for DoD in this new Information Age. The U.S. no longer enjoys the historical geographical protection provided by oceans or the conventional protection provided by its armed forces. DoD has developed a new vulnerabilities which require new thinking and new defenses. Cyberspace is "ageographic" and requires a new paradigm of thinking very different from conventional defense

doctrine. DoD must take action now to remedy its Achilles' Heel of the future.

GLOSSARY

IO Terms[45]:

> Global Information Infrastructure (GII): "the worldwide interconnection of communications networks, computers, databases, and consumer electronics that make vast amounts of information available to users." The GII includes the physical facilities used to store, process, and display information, as well as the personnel who handle the transmitted information.[46]

National Information Infrastructure (NII): "similar to the GII, but relates in scope only to the national information environment."[47]

Defense Information Infrastructure (DII): "the shared interconnected system of computers, data applications, security, people, training, and other support structures serving DoD local, national, and worldwide information needs.. .It includes C2, tactical, intelligence, and commercial information systems used to transmit DoD information."[48]

Information: "facts, data, or instructions in any form or medium."[49]

Information System: "the entire infrastructure, organization, personnel and components that collect, process, store, transmit, disseminate, and act on information."[50]

Information Superiority: "the capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same."[51]

Information Operations (IO): "actions taken to affect adversary information, and information systems, while defending one's own information and information systems."[52]

Information Warfare (IW): "information operations conducted during time of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries."[53]

Command and Control Warfare (C2W): The "application of IW in military operations. C2W specifically attacks and defends the C2 target set."[54]

Information Assurance (IA): "IO that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation."[55]

Intelligence Preparation of the Battlefield (IPB): A deliberate planning process used to assess enemy forces' order of battle, goals, capabilities, strengths, weaknesses, and likely courses of action. The IPB process also includes consideration of terrain, infrastructure, and weather conditions with respect to how they will effect a commander's warfighting capability in a particular operation.

Notes

1. Joint Vision 20 10. Washington: GPO, 1996.

2. Ibid and Draft Joint Publication 3-13, Joint Doctrine for Information Operations, 28 Jan 98, page I-22 and GL- 14. Original definition in Department of Defense Directive S-3600.1, Information Operations, 9 December 96.

3. GAO, Information Security: Computer Attacks at Department of Defense Pose Increasing Risks, On-line. Internet: available from: www.fas.org/irp/gao/aim96084.htm, 22 May 1996.

4. Concept for Future Joint Operations, Expanding Joint Vision 2010, May 1997, page 42.

5. DoD Directive 3600.1, Information Operations, 9 December 1996.

6. Draft Joint Publication 3-l 3, Joint Doctrine for Information Operations, 28 Jan 1998.

7. CJCS Instruction 65 10.0 1 B, Defensive Information Operations Implementation, 30 June 1997.

8. Ibid.

9. Computer Security, Issues & Trends, Vol. IV, No.1, Winter 1998, Computer Security Institute, page 1.

10. Ibid. page 2.

11. Joint Staff/J6K, Information Assurance Division Briefing, Rome Labs Case, November 1997.

12. Prepared Testimony of Jim Christy, AF Investigator before the Senate Government Affairs Committee Permanent Investigations Sub-Committee, 5 June 1996.

13. Joint Staff/J6K, Information Assurance Division Briefing, Rome Labs Case, November 1997.

14. Prepared Testimony of Jim Christy, AF Investigator before the Senate Government Affairs Committee Permanent Investigations Sub-Committee, 5 June 1996.

15. Joint Staff/J6K, Information Assurance Division Briefing, Rome Labs Case, November 1997.

16. Prepared Testimonv of Jim Christy, AF Investigator before the Senate Government Affairs Committee Permanent Investigations Sub-Committee, 5 June 1996.

17. Joint Staff/J6K, Information Assurance Division Briefing, Rome Labs Case, November 1997.

18. Prepared Testimony of Jim Christy, AF Investigator before the Senate Government Affairs Committee Permanent Investigations Sub-Committee, 5 June 1996.

19. Joint Staff/J39 Briefing, IA-The Wav Ahead, March 1998.

20. Ibid.

21. DoD News Briefing, OSD/PA Press Release, 25 February 1998.

22. Glave, James. Wired News, DoD Cracking Team Used Common Bug, 5 March 1998.

23. Lardner, Richard and Hess, Pamela. Pentagon Looks for Answers to Massive Computer Attack, Defense Information and Electronics Report, 13 Feb 1998.

24. Graham, Bradley. 1 1U.S.Military Computer Systems Breached by Hackers This Month, Washington Post, 26 Feb 1998, page 1.

25. Ibid.

26. Joint Staff/J39 Briefing, IA-The Wav Ahead, March 1998.

27. Graham, Bradley. 11 U.S.Military Computer Systems Breached by Hackers This Month, Washington Post, 26 Feb 1998, page 1.

28. Van Derbeken, Jaxon and Doyle, Jim and Martin, Glen. “Hacking Suspect Caught in Cloverdale”,

San Francisco Chronicle, 27 February 1998.

29. Glave, James. Wired News, Analyzer Nabbed in Israel?, 16 March 1998.

30. AntiOnline, "Interview with Makaveli", 2 March 1998.

3 1. Reed, Dan. San Jose Mercury News, "Pentagon Hacker Suspect Tells of Plans for Retaliation", 3 March 1998.

32. DoD News Briefing, OSD/PA Press Release, 25 February 1998.

33. "Report of the Defense Science Board Task Force on Information Warfare-Defense (I W-D)" On-Line. Internet, November 1996. Available from: http:// jya.com/iwd.htm.

34. Campen, Alan D., Col, USAF. "Information War Techniques Supersede Kinetic Weapons" SIGNAL, May 1998, pg 33-36.

35. Ibid, pg.2.

36. Ibid.

37. Ibid, pg. 10.

38. Ibid, pg. 11.

39. Ibid, pg. 12.

40. Ibid, pg14.

41. Ibid, pg15.

42. Army Memorandum. FORSCOM Network Security Improvement Program (NSIP) Action Plan (Draft), pg. 7.

43. Ibid.

44. Critical Foundations, Protecting America's Infrastructures Report of President's Commission on Critical Infrastructure Protection, October 1997.

45. Information Operations: What is the best way to organizationally ysupport the warfighting CINCs?, AFSC Paper, Course 97-4, CDR Racanelli et al.

46. Joint Publication 3-13, Joint Doctrine for Information Operations, 2 July 1997, pg I-24 to I-25.

47. Ibid, pg I-25.

48. Ibid, pg I-25.

49. Ibid, pg I- 17.

50. Ibid, pg I-19.

5 1. Ibid.

52. Ibid, pg I-17.

53. Ibid, pg I-l.

54. Ibid, pg I-3.

55. CJCS Instruction 65 10.01B, Defensive Information Operations Implementation, 30 June 1997, pg GL-9.

Disclaimer

Air Chronicles Home Page | Feedback? Email to editor@cadre.maxwell.af.mil